8Н

УДК 621.396

Ф.Г. Нестерук[1], ***Г.Ф. Нестерук***[2]
[1]Санкт-Петербургский институт информатики и автоматизации РАН, г. Санкт-Петербург, Российская Федерация
[2]Ялтинский университет менеджмента, г. Ялта, АР Крым, Украина
nest_g_p@mail.ru, 08p@mail.ru

К организации интеллектуальной защиты информации на базе адаптивных средств классификации с инкрементным обучением

Рассмотрены вопросы организации системы защиты информации (СЗИ), которая ориентирована на процессы адаптации к динамике компьютерных атак. Показано, что в иерархической модели адаптивной СЗИ нижний уровень, ответственный за оперативную реакцию на динамику внешнего окружения, должен быть интеллектуальным (по аналогии с иммунными механизмами биосистемы). Верхний уровень (соответствует процессам обобщения центральной нервной системы) ориентирован на использование интеллекта администратора безопасности в качестве компонента модели. Каждый из уровней содержит средства нейросетевой классификации с инкрементным обучением, позволяющие повысить оперативность СЗИ за счет минимизации количества кластеров при периодическом выполнении этапов структурной и параметрической оптимизации.

Введение

Актуальность предложенных на обсуждение материалов обусловлена тем, что системы защиты информации (СЗИ), предназначенные для обеспечения безопасности информационно-коммуникационных систем (ИКС), должны реализовать оперативную реакцию в условиях высокой динамики угроз, изменения стратегии компьютерных атак. Одно из решений проблемы – применение интеллектуального подхода к разработке перспективных СЗИ [1], [2].

Одним из требованием к СЗИ для критически важных объектов является *оперативность реакции на угрозы* возникновения деструктивных системных событий. К критически важным объектам ИКС относят техногенные системы, выведение из строя которых может привести к катастрофическим последствиям.

Инкрементное обучение позволяет реализовать адаптацию средств нейросетевой классификации в режиме реального времени [3], что принципиально важно для СЗИ критически важных объектов.

В основе адаптивных средств классификации (АСК) с инкрементным обучением лежит *принцип двойной пластичности*: структурные изменения в биосистеме происходят реже, чем изменения функциональных параметров [4].

Рассматриваемая задача – повышение оперативности АСК согласно принципу двойной пластичности, т.к. одновременно формируется топология и производится обучение нейронной сети (НС). Основная идея нейросетевого классификатора EMANN – первичность эволюции внутренних функциональных параметров НС в процессе обучения и вторичность изменения ее структуры. Повышение точности классификации сопровождается поддержанием минимальной топологии НС [4], [5]. АСК формируются добавлением и/или

изъятием формального нейрона (ФН) без существенного изменения остальных весов межнейронных связей (информационного поля НС). Изменение структуры АСК не сопровождается обучением информационного поля всей НС, а только фрагмента, связанного с упомянутым ФН, что увеличивает оперативность инкрементного классификатора.

Инкрементным обучением с учителем при решении задач классификации характеризуется класс сетей ART, включающий Fuzzy ARTMAP (FAM) [3], [6]. Проблемами сетей ART являются рост числа кластеров в процессе эксплуатации классификатора и явление *пролиферации*. Подобные явления снижают производительность сетей ART и оперативность реакции СЗИ на динамику угроз.

Цель работы – обсуждение подхода к организации интеллектуальной защиты информации на базе АСК с инкрементным обучением. На этапе структурной пластичности помимо увеличения числа кластеров в процессе обучения НС периодически выполняется процедура сокращения их числа за счет удаления малозначащих кластеров и кластеров, сформированных посредством пролиферации.

Модель интеллектуальной СЗИ

Рассмотрим модель интеллектуальной СЗИ в виде иерархии уровней АСК [2].

Знание – структурообразующее понятие, постоянный процесс изменения связей данных. *Информационная база* (ИБ) состоит из взаимосвязанных базы данных (БД), базы знания (БЗ), средств ее разработки и управления, а информационные процессы рассматриваются как субъект-объектное взаимодействие. Для организации субъект-объектного взаимодействия требуются две информационные базы, которые образуют *интеллектуальную базу* [7].

Одна информационная база представляет жизненный опыт – «память», а другая – «текущее состояние» системы. Новые знания возникают в процессе взаимодействия информационных баз и стабилизации их структуры.

Рассмотрим, каким образом концепция интеллектуальной базы соотносится с иерархией уровней АСК в составе СЗИ. Согласно [2], [8] система защиты ИКС может быть представлена двухуровневой иерархической структурой:

– нижний уровень – автоматический за счет наличия интеллектуальной базы, которая самостоятельно набирает опыт эксплуатации в процессе «общения» ИБ «память» и ИБ «текущее состояние» через коммуникационную среду;

– верхний уровень также содержит информационную базу, ориентирован на получение информации о динамике изменения нижнего уровня и не является интеллектуальным и автоматическим, т.к. решение принимает администратор безопасности (он является интеллектуальной базой уровня).

То есть при сохранении двухуровневой иерархии СЗИ, содержащей АСК, назначение и функции уровней СЗИ разные:

– нижний становится интеллектуальным (аналог иммунных механизмов в организме, которые работают оперативно и автоматически, практически без коррекции со стороны головного мозга – центральной нервной системы организма);

– верхний (соответствует процессам запоминания в центральной нервной системе организма, которая работает значительно медленнее) накапливает опыт под контролем и участии администратора безопасности.

Проиллюстрируем изменения в модели СЗИ посредством рис. 1 [7].

В момент создания интеллектуального уровня в него с верхнего уровня иерархии загружают (этап наследования): исходные БД и БЗ, начальные методы их взаимодействия с внешним миром и их собственной коррекции.

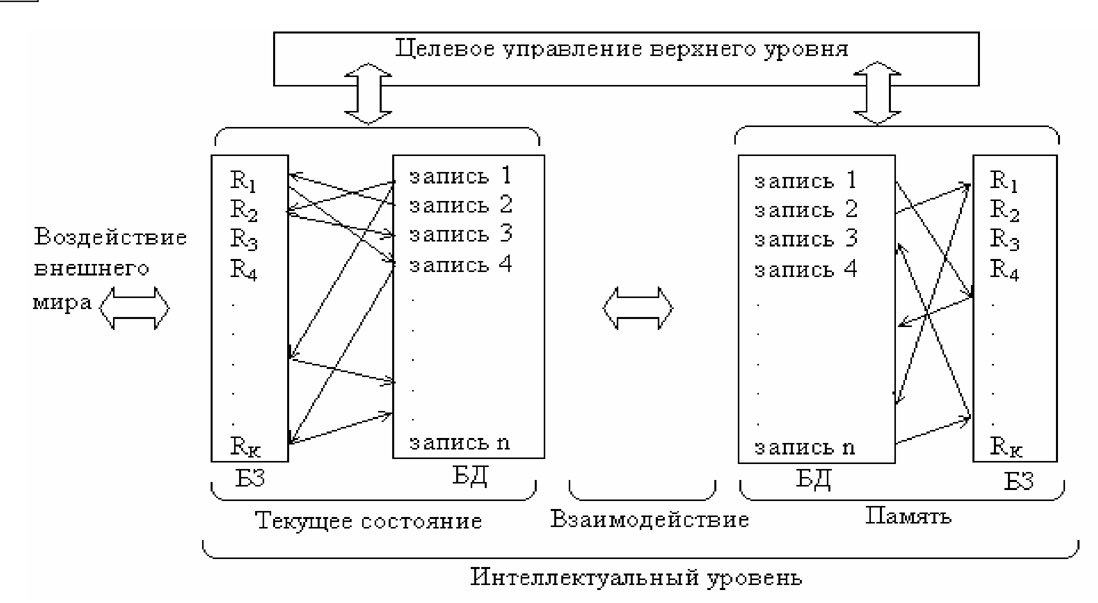


Рисунок 1 – Иерархия адаптивных уровней интеллектуальной СЗИ

Нижний уровень взаимодействует с внешним миром и автоматически изменяется: в ИБ «Текущее состояние» изменяются как БД и БЗ, так и методы взаимодействия с внешним миром и их коррекции (реализуется свойство пластичности). В ИБ «Память» происходят аналогичные изменения, но в результате взаимодействия с ИБ «Текущее состояние» и целевых установок верхнего уровня (администратора безопасности) – в памяти фиксируются существенные изменения (реализуется свойство стабильности).

Верхний иерархический уровень СЗИ получает с нижнего уровня иерархии системы защиты динамику состояний как «памяти» (стабильность), так и «текущего состояния» (пластичность) с целью интеллектуального анализа (посредством АСК) и коррекции структуры СЗИ (посредством методики оптимизации при участии *естественного интеллекта* администратора безопасности ИКС).

Для организации информационной связи с внешним миром необходимы посредники – параметры физической среды, через которые можно судить о динамике воздействия коммуникационной среды ИКС и Интернета. В качестве входных параметров могут выступать:

– статистика ИКС (частота посещения ИКС, анализ сетевых адресов: из каких доменов, частота повторения адресов и пр.);

– статистика операционной системы (открытие, закрытие файлов, операции над файлами, временные параметры, попытки обращения к системным файлам и защищаемым областям памяти и пр.).

Анализ нейросетевых АСК с инкрементным обучением

Проведем анализ архитектурных аспектов сетей FAM и EMANN с сохранением обозначений, принятых в оригиналах материалов [5], [9], [10].

Fuzzy ARTMAP часто реализуют в виде упрощенной модели (рис. 2) [9], полученной комбинацией самообучаемой сети ART с полем преобразования.

FAM состоит из двух уровней узлов (нейронов) с полными связями: M узлов входного слоя F_1, и N узлов соревновательного слоя F_2. Набор вещественных весов $W = \{w_{ij} \in [0,1] : i = 1, 2, ..., M;\ j = 1, 2, ..., N\}$ соответствует F_1-to-F_2 связями. Каждый j-й узел слоя F_2 представляет *категорию распознавания*, которая соответствует вектору-про-

тотипу $w_j = (w_{1j}, w_{2j}, ..., w_{Mj})$. Слой F_2, связанный через обученные ассоциативные связи с 1, …, L узлами, отображает поле преобразования (map field) F^{ab}, где L – число классов в выходном пространстве. Набор бинарных весов $W^{ab} = \{w_{ij}^{ab} \in \{0,1\} : i = 1, 2, ..., N; j = 1, 2, ..., L\}$ связан с F_2-to-F^{ab}связями. Вектор $w_j^{ab} = (w_{j1}^{ab}, w_{j2}^{ab}, ..., w_{jL}^{ab})$ связывает j-й узел слоя F_2 с L узлами выходных классов.

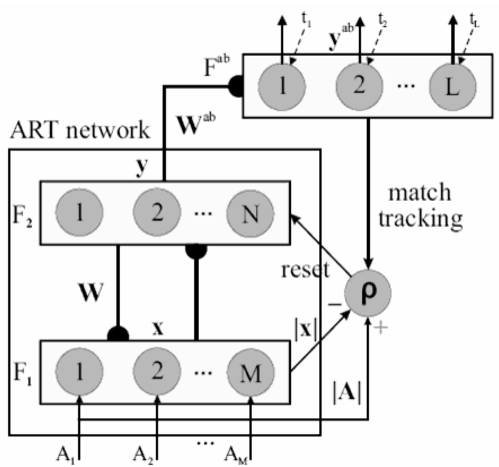


Рисунок 2 – Архитектура Fuzzy ARTMAP

В режиме адаптации FAM использует метод обучения с учителем над нормализованными векторами входного набора обучающей выборки $a = (a_1, a_2, ..., a_m)$, $0 \le a_i \le 1$, согласно выходному вектору (output labels) $t = (t_1, t_2, ..., t_L)$, где t_k = 1, если k – целевая метка класса для вектора ***a***, и t_k = 0 иначе.

M = 2m представляет размерность вектора ***A*** = (***a***, **1** – ***a***), сформированного из вектора ***a*** путем добавления комплементарного фрагмента **1** – ***a***, где **1** обозначен m-мерный вектор, все координаты которого равны 1.

Следующий алгоритм описывает обучение Fuzzy ARTMAP [9]:

1. Инициализация. Изначально все узлы слоя F_2 нейтральны, значения весов w_{ij} = 1, а значения весов w_{jk}^{ab} = 0. Задают начальные значения нормы (*скорости*) обучения $\beta \in [0; 1]$, параметра *выбора* $\alpha > 0$ и параметра *бдительности* $\bar{\rho} \in [0; 1]$. Один из узлов слоя F_2 становится активным по результатам соревнования с другими аналогичными узлами при поступлении входного вектора ***a*** (образца), и затем ассоциируется с одним из узлов в слое F^{ab}.

2. Комплементарное кодирование входного вектора. Когда FAM представлена обучающаяся пара (***a***; ***t***), вектор ***a*** подвергается преобразованию *кодирования дополнением*, которое удваивает число его координат. Полученный таким образом комплементарный входной образец имеет размерность M = 2m и представляется вектором $A = (a, a^c) = (a_1, a_2, ..., a_m; a_1^c, a_2^c, ..., a_m^c)$, где $a_i^c = (1 - a_i)$, $a_i \in [0; 1]$. Параметр бдительности ρ равен базовому значению $\bar{\rho}$.

3. Выбор прототипа (шаблона). Образец ***A*** через слой F_1 передается по взвешенным связям ***W*** к слою F_2. Активация каждого узла j в слое F_2 определяется функцией выбора:

$$T_j(A) = \frac{|A \wedge w_j|}{\alpha + |w_j|}, \quad (1)$$

где $|\cdot|$ – оператор нормы, $\left|w_j\right| \equiv \sum_{i=1}^{M}\left|w_{ij}\right|$, α – заданный пользователем параметр выбора (*choice parameter*), $\wedge$ – нечеткий оператор min, $(A \wedge w_j) \equiv \min(A_i, w_{ij})$.

Слой F_2 формирует бинарный вектор активности $y = (y_1, y_2, ..., y_N)$ по принципу «победитель получает все». Побеждает узел $j=J$ с максимальным значением функции выбора $J = \arg\max\{T_j : j = 1,2,...,N\}$. При этом $y_J = 1, y_j = 0, j \neq J$. Если функции выбора T_j имеют несколько равных максимальных значений, то выбирается узел j с наименьшим значением индекса. Узел J передает *выходной вектор опытного образца* в обратном направлении к слою F_1 для выполнения теста *бдительности* (vigilance test). Тест сравнивает степень *соответствия* (degree of match) между w_J и **A** с параметром *бдительности* (vigilance parameter) ρ:

$$\frac{\left|A \wedge w_j\right|}{M} \geq \rho . \tag{2}$$

Если тестирование успешное, то узел J остается активным, и считают, что имеет место *резонанс*. Иначе, узел J в слое F_2 деактивируется (т.е. T_J устанавливают в 0, пока в сети не представлена следующая обучающая пара (***a***; ***t***)) и исследуют следующий узел J с максимальным значением функции выбора, который может пройти тест бдительности. Если такой узел не обнаружен, то активируется и обучается ранее нейтральный узел в слое F_2.

4. Предсказание класса. Полю преобразования F^{ab} для обучения с учителем категории ***y*** слоя F_2 предъявляется выходной образец ***t***, чтобы инициировать поле преобразования через ассоциативные веса W^{ab}. Слой F^{ab} формирует двоичный вектор активности $y^{ab} = (y_1^{ab}, y_2^{ab}, ..., y_L^{ab})$, в котором наиболее активный узел K выполняет предсказание класса $K = k\ (J)$. Если узел K определил класс входного образца неправильно, то процедура *состязания* (match tracking) увеличивает параметр бдительности ρ до значения, достаточного для стимулирования поиска среди других узлов слоя F_2 (п. 3). Этот поиск продолжается, до тех пор, пока: 1) узел J после дополнительного обучения правильно предскажет класс K и станет активным или 2) активируется нейтральный узел в слое F_2.

5. *Обучение* по входному вектору ***a*** приводит к модификации вектора прототипа w_J, создается ассоциативная связь к полю F^{ab} и вектор прототипа узла J из слоя F_2 модифицируется согласно:

$$w_J^{'} = \beta(A \wedge w_J) + (1-\beta)w_J , \tag{3}$$

где β – параметр *нормы* обучения. Алгоритм может быть настроен на *быстрое обучение* (β = 1) или *замедленное обучение* (0 < β < 1). FAM, использующая комплементарное кодирование и инкрементное обучение, представляет категорию j как m-мерный гиперпрямоугольник Rj, который является достаточно большим, чтобы охватить соответствующий вектор ***a*** обучающей выборки. Новая ассоциация между узлом J из слоя F_2 и узлом K из F^{ab} ($K = k\ (J)$) обучается путем задания веса связи $w_{Jk}^{ab} = 1$ для $k = K$, где K – целевая метка класса для ***a***, и $w_{Jk}^{ab} = 0$, иначе. Если веса ***W*** сходятся для образцов обучающей выборки с заданной точностью, FAM может предсказывать метку класса для каждого входного образца, выполняя п. 2 – 4 без тестов бдительности или соответствия.

Геометрическая интерпретация Fuzzy ARTMAP [10]. Шаблон (прототип), соответствующий активному узлу, называется *активным шаблоном* (помечен литерой *a*), а шаблон нейтрального узла – *нейтральным шаблоном*, который представляется

вектором, все координаты которого равны 1. Нисходящие веса от узла в области F_2^a рассматриваются как *шаблон*. Если имеется активный шаблон w_j^a, соответствующий входным образцам $I^1 = (x(1), x^c(1))$, $I^2 = (x(2), x^c(2))$, …, $I^P = (x(P), x^c(P))$, то согласно правилу обучения FAM w_j^a может быть записан как:

$$w_j^a = \wedge_{i=1}^{P} I^i = (\wedge_{i=1}^{P} x(i), \wedge_{i=1}^{P} x^c(i)) = (\wedge_{i=1}^{P} x(i), \{\vee_{i=1}^{P} x(i)\}^c).$$

Или $w_j^a = (u_j^a, \{v_j^a\}^c)$, где $u_j^a = \wedge_{i=1}^{P} x(i)$ и $v_j^a = \vee_{i=1}^{P} x(i)$. Вектор веса w_j^a в терминах *M*-мерных векторов u_j^a и v_j^a м.б. представлен двумя точками в *M*-мерном пространстве (рис. 3 для $M = 2$) [10].

Геометрическое представление весов может быть расширено на пространство входных образцов. Входной образец $I = (x, x^c)$ можно геометрически интерпретировать прямоугольником с конечными точками (end-points) *x* и *x*, т.е. вектор *I* может быть представлен прямоугольником размера 0 или отдельной точкой *x* в *M*-мерном пространстве.

Размер прямоугольника R_j^a с конечными точками u_j^a и v_j^a принят равным норме вектора $L_1 = v_j^a - u_j^a$, где норма вектора – это сумма абсолютных величин ее компонентов. Итак, можно представлять $w_j^a = (u_j^a, \{v_j^a\}^c)$ как прямоугольник R_j^a с конечными точками u_j^a и v_j^a в *M*-мерном пространстве, а $I = (x, x^c)$ как точку *x* в *M*-мерное пространстве.

В течение процесса обучения FAM «сжатые» представления входных образцов, принадлежащих к набору обучения, формируются в области F_2^a и могут визуализироваться как прямоугольники, соответствующие активированным узлам в F_2^a. Идея соотнесения прямоугольника с кластером (узлом НС) состоит в том, что в пределах его границ разместились соответствующие этому узлу входные образцы. В FAM представления входных образцов, размещенные в слое F_2^a, ассоциируются (are mapped) в ходе обучения с их правильными выходными образцами (метками).

Каждый нисходящий вектора веса w_j^a, соответствующий узлу *j* в слое F_2^a, в *M*-мерном пространстве интерпретируется прямоугольником с конечными точками u_j^a и v_j^a, а входной образец $I = (x, x^c)$ – *M*-мерным вектором входа *x* (рис. 3) [10].

Расстояние *dis(x,* w_j^a*)* между входным образцом *x* и прямоугольником R_j^a, представляющего категорию w_j^a, который не включает *x*, – это минимальное расстояние от *x* до точки, принадлежащей границе прямоугольника R_j^a.

Нейронная сеть EMANN представляется в виде иерархии модулей, в которой вводится операция расширения НС [5]. Каждый модуль – НС с одним скрытым слоем. Входы EMANN соединены со входами всех модулей, что позволяет избежать зависимости новых модулей от имеющихся модулей. Выходы имеющихся модулей соединены со входами введенного модуля, а решение задачи снимается с выходов модуля верхнего уровня. В процессе обучения (параметрическая пластичность) каждый новый модуль должен дополнять существующие и извлекать полезную информацию из модулей более низкого уровня.

Минимальная структура EMANN имеет один ФН в скрытом слое. Количество входов и выходов определяется условиями задачи. Так как начальная структура (информационное поле НС) минимальна, то для поддержания обобщающей способности следует

периодически наращивать информационное поле НС путем добавления ФН и межнейронных связей (структурная пластичность). Также периодически следует избавляться от малозначащих для классификации ФН [5] согласно весовому параметру нейрона (ВПН) – среднее значение весов данного ФН

$ВПН = \frac{\sum_{i=1}^{n} W_i}{n}$, где n – число входов ФН, W_i – значение веса i-й связи.

Вклад ФН в процесс классификации характеризуется близкими к 1 значениями выхода. *Стабильный* ФН, сильно влияющий на результаты классификации, – это нейрон, ВПН которого превышает заданное пороговое значение. Если все ФН модуля – стабильные, то положение разделяющих гиперплоскостей классификатора фиксировано и не изменяется в процессе обучения НС (модуль не совершенствуется). Поэтому EMANN поддерживает в модуле ряд *нестабильных* ФН, которые характеризуются малым значением ВПН, формируют на выходе значения в диапазоне ±0,5, а положение связанных с ними гиперплоскостей может изменяться в процессе обучения НС. *Бесполезный* ФН определен как нейрон, ВПН которого меньше значения *порога полезности*. Удаление бесполезных ФН мало влияют на функции модуля.

Удаление ФН предшествует добавлению нового модуля. При добавлении ФН в скрытый слой модуля его веса задают по принципу комплементарности остальным ФН данного модуля. Для содействия другим ФН с низким значением ВПН новые ФН инициализируют, чтобы их выходы максимально отличались от выходов остальных ФН за счет комбинации весов, имеющей максимальное количество инверсий знаков.

Эволюция каждого модуля включает 4 этапа [4].

Этап подъема – добавление ФН при превышении значения константы подъема. Этап завершается, если один из ФН становится стабильным, но хотя бы один вес связей между входами НС и ФН текущего модуля превышает порог стабилизации – гарантия, что хотя бы один из новых ФН участвует в классификации.

Этап улучшения – при стабилизации в модуль добавляется новый ФН и в процессе обучения отслеживается улучшение решения задачи (по мере увеличения числа стабильных ФН точность решения задачи улучшается). Этап улучшения завершается, если ни один из ФН не стабилизировался за время, называемое *параметром ожидания*.

Этап сокращения – удаление ФН, ВПН которых меньше *порога полезности*.

Этап восстановления – адаптируют модуль на малом числе эпох обучения для восстановления точности решения задачи, сниженной на этапе сокращения.

После завершения описанного цикла структура модуля фиксируется, и EMANN переходит к построению нового модуля более высокого уровня (модуль будет оставлен при условии, что его добавление улучшит точность решения задачи). Как достоинство можно отметить наличие механизма регуляции числа ФН: EMANN увеличивает число ФН по мере роста сложности задачи, что помогает найти оптимальное по сложности решение задачи.

Модификация алгоритма FAM

Модификация алгоритма FAM заключается во введении этапов *сокращения и восстановления* по аналогии с подходом EMANN, что позволит уменьшить количество малозначащих для классификации ФН с последующим восстановлением точности в процессе обучения. Сокращение числа малозначащих или идентичных кластеров в FAM приведет к повышению оперативности интеллектуальных СЗИ.

Однако используемый в EMANN критерий ВПН не может быть применен в FAM, т.к. шаблон (кластер) $w_j = (w_{1j}, w_{2j}, ..., w_{Mj})$, представляющий j-ю *категорию распознавания*, при комплементарном кодировании входных параметров $a_i^c = (1 - a_i)$ характеризуется постоянным значением весового параметра ФН для всех j.

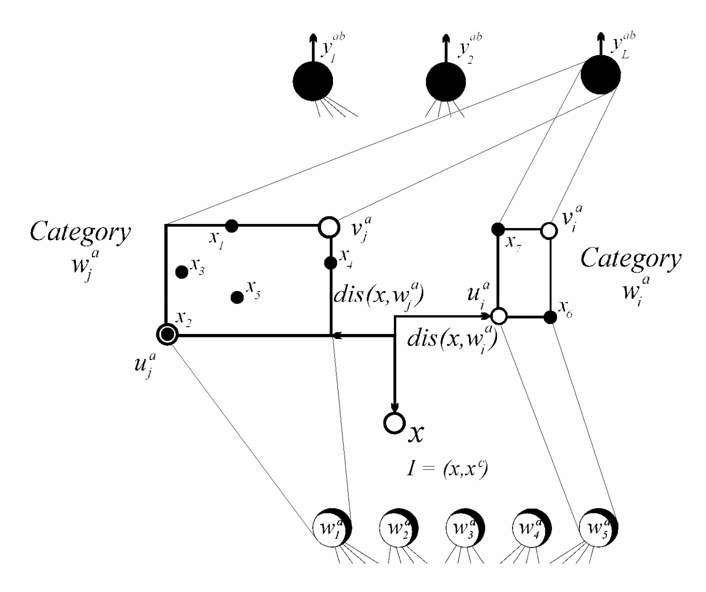
Предлагается на обучающей (и тестовой) выборке набирать статистические сведения, например, о взаимосвязи входных векторов с конкретными узлами слоя F_2 – победителями соревнования. Можно фиксировать число k_j входных векторов, соответствующее каждому j-му кластеру. Кластер удаляется, если его $k_j < \eta$ (степени востребованности кластера) и качество классификации ухудшилось на величину $q < \mu$ (допустимое ухудшение).

Кроме того, для выявления повторяющихся кластеров следует определять расстояние Δ_{ij} между i-м и j-м шаблонами, представляющими различные *категории распознавания*, $i \neq j$. Кластер можно убрать, если $\Delta_{ij} < \kappa$ (степень различия кластеров) и качество классификации ухудшилось на величину $q < \mu$ (допустимое ухудшение). Среди повторяющихся кластеров в качестве базового для сравнения следует выбирать кластер, у которого число k_j входных векторов, соответствующее j-му кластеру максимально.

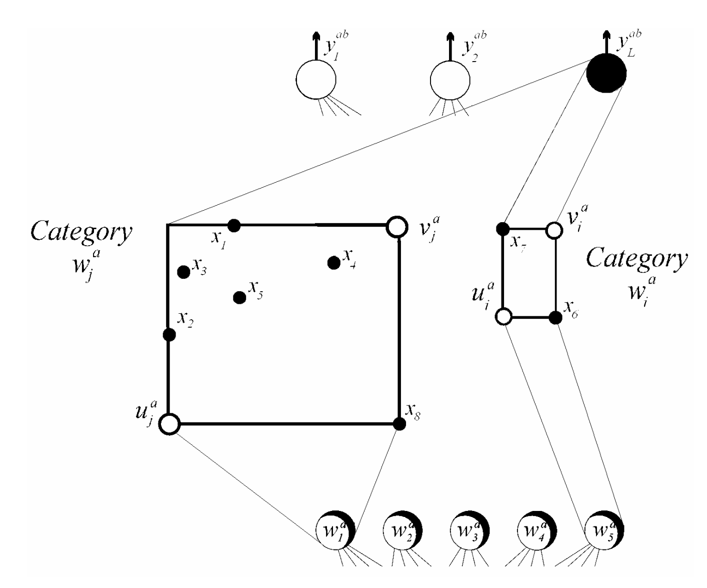
Рис. 3 иллюстрирует процесс сокращения числа кластеров. В процессе обучения классификатора сформированы две категории w_i^a и w_j^a, $i \neq j$. При поступлении нового входного образца $I = (x, x^c)$ определяются его удаленность $dis(x, w_i^a)$ и $dis(x, w_j^a)$ от каждого из кластеров (рис. 3 а).

В режиме «быстрого» обучения согласно (3) более близкий j-й кластер увеличивается и включает в себя входной образец (рис. 3 б).

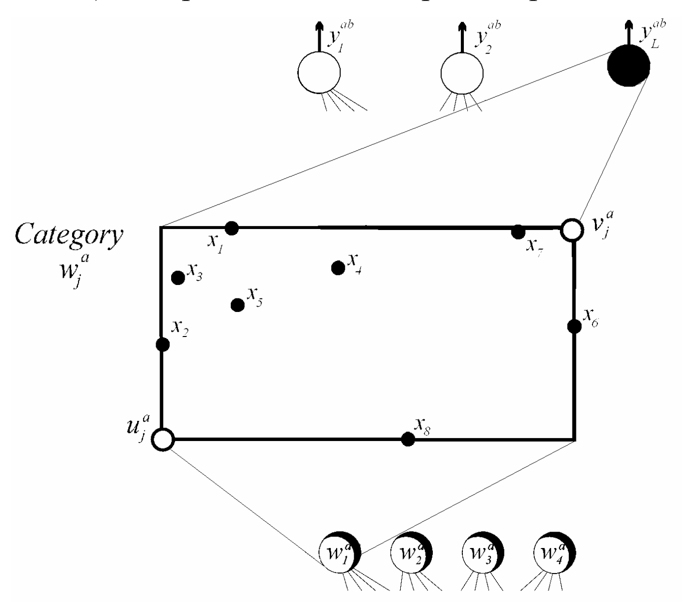
Рис. 3 б иллюстрирует случай, когда две категории распознавания, близкие во входном пространстве, определяют один класс y_L^{ab}. В качестве базовой категории выбирается кластер w_j^a, у которого большее число входных векторов $k_j = 6$ по сравнению с кластером w_i^a ($k_i = 2$).



а) отнесение образца $I=(x,x^c)$ к j-му кластеру



б) выбор базового кластера для сравнения



в) результат сокращения количества кластеров

Рисунок 3 – Иллюстрация процесса сокращения количества кластеров

После удаления кластера w_i^a следует провести цикл обучения только на входных векторах, соответствующих удаленному *j*-му кластеру. Так после удаления кластера w_i^a и обучения НС на входных образцах x_6 и x_7, ранее входивших в удаленный кластер, увеличившийся в размерах кластер w_j^a обучился распознаванию образцов x_6 и x_7 (рис. 3 в).

Отметим, что кандидата на удаление среди кластеров можно выбирать по ряду других критериев, к примеру по максимальному числу ошибочных классификаций.

Выводы

Широкое использование сетей ART позволяет считать актуальным поиск подходов, позволяющих улучшить их эксплуатационные характеристики и не в последнюю очередь скорость выполнения операции классификации. Реализация в инкрементных

классификаторах ART процедуры сокращения малозначащих и повторяющихся кластеров позволяет увеличить производительность построенных на их основе адаптивных средств защиты информации как в режиме работы, так и в процессе обучения, а следовательно, в полной мере реализовать режим функционирования СЗИ, близкий к реальному масштабу времени.

Литература

1. Нестерук Г.Ф. Информационная безопасность и интеллектуальные средства защиты информационных ресурсов. (Иммунология систем информационных технологий) / Нестерук Г.Ф., Осовецкий Л.Г., Харченко А.Ф. – СПб. : Изд-во СПбГУЭФ, 2003. – 364 с.
2. Адаптивные средства обеспечения безопасности информационных систем / [Нестерук Ф.Г., Суханов А.В., Нестерук Л.Г. , Нестерук Г.Ф.] ; под ред. Л.Г. Осовецкого. – СПб. : Изд-во Политехнического университета, 2008. – 626 с.
3. Carpenter G.A. ARTMAP: Supervised Real-Time Learning and Classification of Nonstationary Data by a Self-Organizing Neural Networ / Carpenter G.A., Grossberg S., & Reynolds J.H. // Neural Networks. – 1991. – № 4. – P. 565-588.
4. Salom T. An algorithm for self-structuring neural net classifiers / T. Salom, H. Bersini // Proc. 2nd IEEE Conf. On Neural Network (ICNN'94). – 1994. – P. 1307-1312.
5. Искусственные иммунные системы и их применение / [под ред. Д. Дасгупты ; пер. с англ. под ред. А.А. Романюхи]. – М. : ФИЗМАТЛИТ, 2006. – 344 с.
6. Fuzzy ARTMAP: An adaptive resonance architecture for incremental learning of analog maps / [G.A. Carpenter, S. Grossberg, N. Markuzon и др.] // Proc. of the International Joint Conference on Neural Network. – 1992.
7. Лачинов В.М. Информодинамика или Путь к Миру открытых систем / В.М. Лачинов, А.О. Поляков. – [2-е изд., перераб. и доп.] – СПб. : Издательство СПбГТУ, 1999.
8. Организация иерархической защиты информации на основе интеллектуальных средств нейронечеткой классификации / Нестерук Г.Ф., Молдовян А.А., Нестерук Ф.Г. [и др.] // Вопросы защиты информации. – 2005. – № 3. – С. 16-26.
9. A what-and-where fusion neural network for recognition and tracking of multiple radar emitters / Granger E., Rubin M. A., Grossberg S., Lavoie P. – Neural Networks. – Vol. 3. – 2001. – P. 325-344.
10. Bharadwaj M. Semi-Supervised Learning in Exemplar Based Neural Networks / M. Bharadwaj // A thesis submitted of the requirements for the degree of Master of Science in the Department of Electrical and Computer Engineering in the College of Engineering at the University of Central Florida, (Orlando, Florida, 2003). – 218 p.

Ф.Г. Нестерук, Г.П. Нестерук

До організації інтелектуального захисту інформації на базі адаптивних класифікаторів з інкрементним навчанням

Розглянуті питання організації системи захисту інформації, яка орієнтована на процеси адаптації до динаміки комп’ютерних атак. Показано, що в ієрархічній моделі адаптивного захисту нижній рівень, відповідальний за оперативну реакцію на динаміку зовнішнього оточення, має бути інтелектуальним (за аналогією з імунними механізмами біологічної системи). Верхній рівень (відповідає процесам узагальнення центральної нервової системи) орієнтований на використання інтелекту адміністратора безпеки як компонента моделі. Кожен з рівнів містить нейромережний класифікатор з інкрементним навчанням, який дозволяє підвищити швидкість класифікації за рахунок мінімізації кількості кластерів при періодичному виконанні етапів структурної і параметричної оптимізації.

Ph.G. Nesteruk, G.Ph. Nesteruk

Intellectual Protection of the Information on the Base of Adaptive Classifiers With the Incremental Training

The organization of the system of safety, which is oriented to the processes of adaptations to the dynamics of computer attacks is considered. It is marked that a lower level of hierarchical model of adaptive defense must be intellectual (by analogy with the immune mechanisms of the biological system). A top level is oriented to the use of intellect of system administrator as a component of model (by analogy with the processes of generalization of CNS). Each of levels contains neural classifier with the incremental teaching. A similar classifier enables to increase speed of classification due to minimization of amount of clusters at periodic implementation of the stages of structural and parametric optimization.

Статья поступила в редакцию 31.05.2010.